

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2003 年 3 月 27 日 (27.03.2003)

PCT

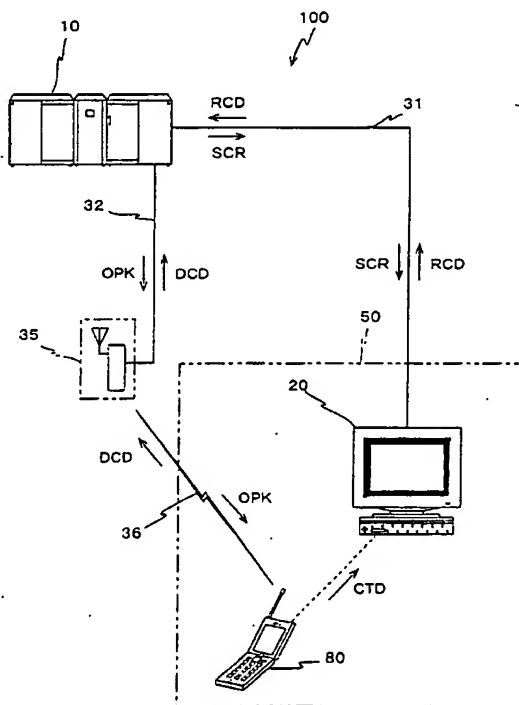
(10) 国際公開番号
WO 03/025771 A1

- (51) 国際特許分類: G06F 15/00, H04L 9/32 (74) 代理人: 柴田五雄(SHIBATA, Itsuo); 〒104-0031 東京都中央区京橋1-19-4 TAF京橋ビル7階 Tokyo (JP).
- (21) 国際出願番号: PCT/JP01/08010
- (22) 国際出願日: 2001 年 9 月 14 日 (14.09.2001)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): 株式会社 鷹山 (YOZAN INC.) [JP/JP]; 〒155-0031 東京都世田谷区北沢3-5-18 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 清松久典 (KIY-OMATSU, Hisanori) [JP/JP]; 〒155-0031 東京都世田谷区北沢3-5-18 株式会社 鷹山内 Tokyo (JP).
- (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ユーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[続葉有]

(54) Title: AUTHENTICATION TERMINAL DEVICE, RECEPTION TERMINAL DEVICE, AUTHENTICATION SERVER, AUTHENTICATION METHOD AND AUTHENTICATION SYSTEM

(54) 発明の名称: 認証端末装置、受付端末装置、認証サーバ、認証方法、及び認証システム



(57) Abstract: An authentication terminal device (80) ciphers user identification data predetermined for identifying a user and password data determined in relation to the user identification data by using a cipher key created for each service provision request. Subsequently, the authentication terminal device (80) transmits authentication data (CTD) containing the ciphered user identification data and password data and deciphering data (DCD) containing cipher key information reflecting the cipher key. Moreover, a service providing system having an authentication server (10) and a reception terminal device (20) deciphers the ciphered user identification data and password data on the basis of the cipher key information, and collates the deciphered user identification data and the deciphered password data to authenticate the user.

[続葉有]

WO 03/025771 A1



添付公開書類：
一 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

認証端末装置（80）が、利用者を特定するために予め定められた利用者識別データ及び前記利用者識別データに関連して定められた暗証データを、サービス提供要求ごとに作成した暗号鍵を用いて暗号化する。引き続き、認証端末装置（80）が、暗号化された利用者識別データ及び暗証データを含む認証用データ（CTD）、及び暗号鍵を反映した暗号鍵情報を含む復号用データ（DCD）を送信する。そして、認証サーバ（10）及び受付端末装置（20）を備えるサービス提供システムが、暗号鍵情報に基づいて、暗号化された利用者識別データ及び暗証データを復号化した後、復号化された利用者識別データと復号化された暗証データとを照合して、利用者の認証を行う。

明 細 書

認証端末装置、受付端末装置、認証サーバ、認証方法、及び認証システム

技術分野

本発明は、認証端末装置、受付端末装置、認証サーバ、認証方法、及び認証システムに係り、より詳しくは、クレジットサービスやデビットカードサービスにおける支払金の決済時等に行われるサービス利用者の認証にあたって使用される認証用端末、受付端末装置、認証サーバ、及び認証方法、並びに該認証方法を使用する認証システムに関する。

背景技術

近年、クレジットサービスやデビットカードサービスにおける支払金の決済等といった、セキュリティを確保すべきサービスが広く利用されている。こうしたセキュリティを確保すべきサービスを実施する場合には、サービス利用者が、確かにサービスの提供を受ける権限のある者であることの確認、すなわち、本人認証が重要となる。かかる本人認証のため、従来は、以下のような方法を使用していた。

例えばクレジットサービスの場合には、店舗における商品の購入にあたり、その販売店において、店員が決済伝票を作成する。この決済伝票は、サービスの利用を希望する者（以下、「サービス利用希望者」という）が持っているクレジットカードに表示及び記憶されている利用できる者すなわち支払いを行うことになる者（以下、「サービス利用可能者」という）に関する識別子（以下、「利用者識別子」という）に基づいて作成される。そして、その決済伝票にサービス利用希望者が署名する。この後、店員が、クレジットカードに記されたサー

ビス利用可能者の署名と決済伝票における署名とを照合する方法によって、本人認証が行われていた。なお、現状においては、クレジット決済端末が、クレジットカードに記憶された利用者識別子を読み取って、決済伝票を作成する方法が主流となっている。

また、デビットカードサービスの場合には、店舗における商品の購入にあたり、その販売店に設置されたデビットカード決済端末によりデビットカードから利用者識別子を読み取り、サービス利用希望者が暗証番号をマニュアル入力する。そして、利用者識別子と暗証番号とを照合する方法により、本人認証が行われていた。

以上のような従来例において決済端末を使用する場合には、本人認証に用いられる利用者識別子を決済端末に供給することになる。このため、決済端末から利用者識別子が窃取され、クレジットカードやデビットカードが偽造される可能性があった。クレジットサービスの場合、クレジットカードが偽造され、偽造者によるクレジットカードへの署名がなされてしまうと、正規のサービス利用可能者が不正使用に気が付き、偽造されたクレジットカードに関する利用者識別子に対するサービス提供の停止を請求するまで、不正使用を防ぐ方策が無い。

一方、デビットカードの場合には、カードが偽造されただけでは不正使用がされることはない。しかし、店頭で暗証番号を入力することから、容易に暗証番号を盗み見られる可能性がある。

さらに、現状のネットワークによる決済等においては、利用者識別子等の本人認証用データを、セキュリティが確認されていないインターネットを介して送信している。この場合、利用者識別子等の本人認証用データを、平文のままネットワークに提供する方法を採用するのでは、本人認証データの窃取に対して高いセキュリティを確保することはできない。このため、現状のネットワークによる決済サービス等は、個人情報の保護の点に課題を抱えているといえ

る。

このため、指紋等の一身専属的な身体特徴を用いた本人認証システムも提案されているが、認証精度が高いとはいえず、また、システムの構成が複雑化することから、結果的にシステム導入コストが高いものになってしまう。

本発明は、上記の事情のもとでなされたものであり、その第1の目的は、簡便な構成で、高いセキュリティを実現可能な認証システム及び認証方法を提供することにある。

また、本発明の第2の目的は、高いセキュリティを実現可能な認証システムの構築に適した、認証端末、受付端末、及び認証サーバを提供することにある。

発明の開示

本発明は、第1の観点からすると、サービスの利用者がサービス提供要求をするとき、前記利用者の認証用情報を、受付端末装置及び認証サーバを含むサービス提供システムへ向けて出力する認証端末装置であって、前記利用者を特定するために予め定められた利用者識別データを記憶する記憶手段と；前記利用者識別データに関連して定められた暗証データを入力する暗証データ入力手段と；前記サービス提供要求ごとに暗号鍵を作成し、前記利用者識別データ及び前記暗証データを、前記暗号鍵を用いて暗号化する第1暗号化手段と；前記暗号化された利用者識別データ及び暗証データ、並びに前記暗号鍵を反映した暗号鍵情報から成る前記認証用情報の一部を含む第1データを前記受付端末へ伝達するとともに、前記認証用情報の残りを含む第2データを前記認証サーバへ伝達する伝達手段と；を備える認証端末装置である。

これによれば、サービス提供要求にあたって、第1暗号化手段が、サービス提供要求ごと暗号鍵を作成し、その作成された暗号鍵を用いて、記憶手段に記憶された利用者識別データと、利用者による入力手段の操作により指示された暗証データとを暗号化する。そして、伝達手段が、暗号化された利用者識別デ

ータ、及び暗証番号等の暗証データ、並びに暗号鍵を反映した暗号鍵情報から成る認証用情報の一部を含む第1データを受付端末へ伝達するとともに、認証用情報の残りを含む第2データを認証サーバへ伝達する。

したがって、認証端末装置から、利用者識別データ及び暗証データをサービス提供システムへ通知するために、平文のままネットワーク等に供給することがなくなるので、利用者識別データ及び暗証データといった本人認証用データを平文のままネットワーク等に供給することによるセキュリティの低下を防止することができる。また、サービス提供要求ごとに暗号鍵を作成するので、1つの暗号鍵を固定的に使用することによるセキュリティの低下を防止することができる。さらに、本人認証のために必要な認証用情報を2分割し、一方を受付端末装置へ伝達し、他方を認証サーバへ伝達するので、受付端末装置には、利用者識別データ及び暗証データといった認証用データの一部又は全部が暗号化された態様でのみ供給され、店頭等に設置される受付端末装置からの利用者識別データや暗証データの窃取を防止することができる。こうして、認証用データの窃取に対して高いセキュリティを実現することができる。

本発明の認証端末装置では、前記第1データを、前記暗号化された利用者識別データ及び暗証データを含む認証用データとし、前記第2データを、暗号鍵情報を含む復号用データとすることができる。

また、本発明の認証端末装置では、前記サービス提供システムから供給された公開鍵を用いて、前記暗号鍵を暗号化して前記暗号鍵情報を作成する第2暗号化手段を更に備える構成とすることができる。かかる場合には、暗号鍵を、窃取者による復号化が実質的に不可能な公開鍵による暗号化を更に行って、その公開鍵の作成元であるサービス提供システムに通知するので、セキュリティを更に向上することができる。

また、本発明の認証端末装置では、前記受付端末装置が、前記第1データを前記認証サーバに送信するとき、前記サービス提供要求を特定するイベント識

別データを生成するイベント識別データ生成手段を更に備える構成とし、前記第1データが前記イベント識別データを更に含むとともに、前記第2データが前記イベント識別データを更に含むこととすることができる。かかる場合には、認証サーバが、イベント識別データをキーとして、同一のサービス提供要求に応じた受付端末装置からの第1データと認証端末装置からの第2データとの関連付けを行い、互いに関連している第1データ及び第2データを1組のデータとして、該1組のデータに含まれる暗号鍵情報に基づいて、やはりその1組のデータに含まれる暗号化された利用者識別データ及び暗証データの復号化を行う。したがって、本人認証用のために必要な認証用情報が2分割された態様に到着しても、認証サーバは、これら2分割された認証用情報を、同一のサービス提供要求に係る認証用情報として関連付けることができ、確実に本人認証を行うことができる。

また、本発明の認証端末装置では、前記伝達手段が、前記受付端末装置との間における第1の経路を介する通信を制御する第1通信制御手段と；前記認証サーバとの間における、前記第1の経路とは異なる第2の経路を介する通信を制御する第2通信制御部と；を備える構成とすることができる。かかる場合には、第1データの通信経路と第2データの通信経路とが別々に設定されるので、1つの通信経路から得た情報のみでは、利用者識別データや暗証データを悪用できる態様で窃取することができない。したがって、認証に関するセキュリティを向上することができる。

この場合、前記受付端末装置との間の通信を近距離無線通信とし、前記認証サーバとの間の通信を、移動体通信網を介した通信とすることができる。

また、本発明の認証端末装置では、前記第1データを画像パターンに変換する画像パターン作成装置を更に備えるとともに、前記伝達手段が、前記第1データが変換された画像パターンを表示する表示装置と；前記認証サーバとの間における通信を制御する第1通信制御部と；を備える構成とすることができる。

かかる場合にも、利用者識別データ及び暗証データが暗号化されて伝達されるとともに、第1データの伝達経路と第2データの伝達経路とが別々に設定されるので、1つの伝達経路から得た情報のみでは、利用者識別データや暗証データを悪用できる態様で窃取することができない。また、受付端末装置には、利用者識別データ及び暗証データといった本人認証用データの一部又は全部が暗号化され、かつ、バーコード等のように一目見ただけではその意味内容を認識することができない画像パターン化された態様で供給されるのみである。したがって、店頭等に設置される受付端末装置からの利用者識別データや暗証データの窃取を防止することができる。したがって、本人認証に関するセキュリティを向上することができる。

ここで、前記画像パターン作成装置が、前記認証サーバにから前記第1通信制御部を介して指定された手順に従って、前記第1データから前記画像パターンへの変換を行うこととすることができる。

本発明は、第2の観点からすると、本発明の認証端末装置との間で通信により情報の伝達を行う受付端末装置であって、前記認証端末装置との間の通信を制御する第3通信制御部と；前記認証端末装置から受信した前記第1データを含む受付データを作成する受付データ作成手段と；前記認証サーバとの間の通信を制御し、前記受付データを前記認証サーバへ送信する第4通信制御部と；を備える受付端末装置である。

本発明は、第3の観点からすると、前記第1データを画像パターンに変換する本発明の認証端末装置との間で情報の伝達を行う受付端末装置であって、前記認証端末装置の表示装置に表示された、前記第1データに応じた画像パターンを読み取って、前記第1データに変換する画像パターン読取手段と；前記第1データを含む受付データを作成する受付データ作成手段と；前記認証サーバとの間の通信を制御し、前記受付データを前記認証サーバへ送信する第2通信制御部と；を備える受付端末装置である。

また、本発明は、第4の観点からすると、本発明の認証端末装置とイベント識別データを含む第2データの通信を行う認証サーバであって、前記受付端末装置との間の通信を制御し、前記第1データを含む受付データを受信する第1データ通信制御部と；前記認証端末装置との間の通信を制御し、前記第2データを受信する第2データ通信制御部と；前記第1データと、前記第1データに含まれるイベント識別データと同一のイベント識別データを含む第2データとを1組のデータとして、前記1組のデータに含まれる前記暗号化された利用者識別データ及び暗証データを、前記1組のデータに含まれる暗号鍵情報を用いて復号化する復号化手段と；前記復号化手段により復号化された前記利用者識別データと前記暗証データとを照合し、前記取引者に関する認証を行う認証手段と；を備える認証サーバである。

これによれば、復号化手段が、イベント識別データをキーとして、受付端末装置から第1データ通信制御装置を介して受信した第1データと、認証端末から第2データ通信制御装置を介して受信した第2データとの関連付けを行って1組のデータとし、該1組のデータに含まれる前記暗号化された利用者識別データ及び暗証データを、やはりその1組のデータに含まれる暗号鍵情報を用いて復号化する。そして、認証手段が、復号化手段により復号化された利用者識別データと暗証データとを照合し、前記サービス利用者に関する認証を行う。したがって、高いセキュリティを有しつつ、確実に本人認証を行うことができる。

本発明の認証サーバでは、前記認証端末装置が前記暗号鍵を暗号化して前記暗号鍵情報を作成する際に用いる公開鍵を、所定の個人鍵に基づいて作成し、前記第2データ通信制御装置を介して前記公開鍵を前記認証端末装置に供給する公開鍵作成手段を更に備え、前記復号化手段は、前記個人鍵を用いて前記暗号鍵情報を復号化し、復号化された前記暗号鍵を用いて、前記暗号化された利用者識別データ及び暗証データを復号化する構成とすることができる。かかる

場合には、公開鍵によって作成された公開鍵が、第2データ通信制御手段を介して、認証端末装置に供給される。そして、認証端末装置において、利用者識別データ及び暗証データの暗号化に用いられた暗号鍵が、認証サーバの公開鍵によって暗号化され、その公開鍵の作成元であるサービス提供システムに通知される。このため、セキュリティを更に向上することができる。

また、本発明の認証サーバでは、前記認証端末装置との間の通信を、移動体通信網を介した通信とすることができる。

本発明の認証方法は、第5の観点からすると、サービスの利用者による、受付端末装置及び認証サーバを含むサービス提供システムに対するサービス提供要求にあたり、前記利用者の認証を行う認証方法であって、前記利用者が、予め定められた利用者識別データに関連して定められる暗証データを入力する暗証データ入力ステップと；前記サービス提供要求ごとに、暗号鍵を生成する暗号鍵生成ステップと；前記暗号鍵を用いて、前記利用者識別データ及び前記暗証データを暗号化する第1暗号化ステップと；前記第1暗号化ステップにおいて暗号化された利用者識別データ及び暗証データ、並びに前記暗号鍵を反映した暗号鍵情報から成る認証用情報の一部を含む第1データを前記受付端末装置へ伝達するとともに、前記認証用情報の残りを含む第2データを前記認証サーバへ伝達する認証用情報伝達ステップと；前記第1データを受けた前記受付端末装置が、前記第1データを含む受付データを前記認証サーバへ送信する受付データ送信ステップと；前記第2データ及び前記受付データを受けた前記認証サーバが、前記利用者の認証を行う認証ステップと；を含む認証方法である。

これによれば、暗証データ入力ステップにおいて入力された暗証データ及び予め定められた利用者識別データが、暗号鍵生成ステップにおいてサービス提供要求のたびに新たに作成された暗号鍵により、第1暗号化ステップにおいて暗号化される。引き続き、認証用データ送信ステップにおいて、第1暗号化ステップにおいて暗号化された利用者識別データ及び暗証データ、並びに暗号鍵

を反映した暗号鍵情報から成る認証用情報の一部を含む第1データを受付端末装置へ伝達するとともに、前記認証用情報の残りを含む第2データを前記認証サーバへ伝達する。次に、受付データ送信ステップにおいて、第1データを受けた受付端末装置が、第1データを含む受付データを認証サーバへ送信する。そして、認証ステップにおいて、認証サーバが、暗号鍵情報に基づいて、暗号化された利用者識別データ及び暗証データを復号化し、復号化された利用者識別データと復号化された暗証データとを照合して、利用者の認証を行う。したがって、利用者識別データ及び暗証データといった本人認証用データを平文のままネットワーク等に供給することによるセキュリティの低下を防止することができるとともに、1つの暗号鍵を固定的に使用することによるセキュリティの低下を防止することができる。さらに、本人認証のために必要な認証用情報を2分割し、一方を受付端末装置へ伝達し、他方を認証サーバへ伝達するので、受付端末装置には、利用者識別データ及び暗証データといった認証用データの一部又は全部が暗号化された態様でのみ供給され、店頭等に設置される受付端末装置からの利用者識別データや暗証データの窃取を防止することができる。こうして、本人認証用データの窃取に対して高いセキュリティを実現することができる。

本発明の認証方法では、前記サービス提供システムから供給された公開鍵を用いて、前記暗号鍵を暗号化して前記暗号鍵情報を作成する第2暗号化ステップを更に含むことができる。

また、本発明の認証方法では、前記サービス提供要求を特定するイベント識別データを生成するイベント識別データ生成ステップを更に含み、前記第1データは前記イベント識別データを更に含むとともに、前記第2データは前記イベント識別データを更に含むこととすることができる。

ここで、前記認証ステップが、前記認証サーバが、前記第1データと、前記第1データに含まれるイベント識別データと同一のイベント識別データを含む

第2データとを1組のデータとして、前記1組のデータに含まれる前記暗号化された利用者識別データ及び暗証データを、前記1組のデータに含まれる暗号鍵情報を用いて復号化する復号化ステップと；前記復号化ステップにおいて復号化された前記利用者識別データと前記暗証データとを照合する照合ステップと；を含むこととすることができる。

また、本発明の認証方法では、前記認証用データ送信ステップでは、前記第1データが第1の経路を介して前記受付端末装置へ伝達され、前記第2データが前記第1の経路とは異なる第2の経路を介して前記認証サーバへ伝達されることとすることができる。

また、本発明の認証方法では、前記暗号鍵情報が、前記認証サーバにおいて管理される個人鍵に基づいて作成された公開鍵を用いて暗号化されたものであり、前記復号化ステップでは、前記個人鍵を用いて前記暗号鍵情報を復号化し、復号化された前記暗号鍵を用いて、前記暗号化された利用者識別データ及び暗証データを復号化することとすることができる。

本発明は、第6の観点からすると、サービスの利用者によるサービス提供要求にあたり、前記利用者の認証を行う認証システムであって、前記利用者を特定するために予め定められた利用者識別データ及び前記利用者識別データに関連して定められた暗証データを、前記サービス提供要求ごとに作成した暗号鍵を用いて暗号化し、前記暗号化された利用者識別データ及び暗証データ、及び前記暗号鍵を反映した暗号鍵情報から成る認証用情報の一部を含む第1データ、及び前記認証用情報の残りを含む第2データを伝達する認証端末装置と；前記認証用データを受け、前記第1データを含む受付データを作成して送信する受付端末装置と；前記受付データ及び前記第2データを受け、前記暗号鍵情報に基づいて前記暗号化された利用者識別データ及び暗証データを復号化し、復号化された利用者識別データと復号化された暗証データとを照合して、前記利用者の認証を行う認証サーバと；を備える認証システムである。

これによれば、認証端末装置が、利用者を特定するために予め定められた利用者識別データ及び利用者識別データに関連して定められた暗証データを、サービス提供要求ごとに作成した暗号鍵を用いて暗号化する。引き続き、認証端末装置が、暗号化された利用者識別データ及び暗証データ、及び前記暗号鍵を反映した暗号鍵情報から成る認証用情報の一部を含む第1データを受付端末装置へ伝達するとともに、認証用情報の残りを含む第2データを認証サーバへ伝達する。次に、第1データを受けた受付端末装置が、第1データを含む受付データを認証サーバへ送信する。そして、認証サーバが、暗号鍵情報に基づいて、暗号化された利用者識別データ及び暗証データを復号化した後、復号化された利用者識別データと復号化された暗証データとを照合して、利用者の認証を行う。すなわち、本発明の認証システムでは、本発明の認証方法を使用して、本人認証をすることができる。したがって、利用者識別データ及び暗証データといった本人認証用データを平文のままネットワーク等に供給することによるセキュリティの低下を防止することができるとともに、1つの暗号鍵を固定的に使用することによるセキュリティの低下を防止することができる。さらに、本人認証のために必要な認証用情報を2分割し、一方を受付端末装置へ伝達し、他方を認証サーバへ伝達するので、受付端末装置には、利用者識別データ及び暗証データといった認証用データの一部又は全部が暗号化された態様でのみ供給され、店頭等に設置される受付端末装置からの利用者識別データや暗証データの窃取を防止することができる。こうして、本人認証用データの窃取に対して高いセキュリティを実現することができる。

本発明の認証システムでは、前記第1データを、前記暗号化された利用者識別データ及び暗証データを含む認証用データとするとともに、前記第2データを、暗号鍵情報を含む復号用データとすることができる。

なお、本発明の認証システムの認証端末装置として、本発明の認証端末装置を使用することができる。

すなわち、本発明の認証システムでは、前記認証端末装置が、前記利用者を特定するために予め定められた利用者識別データを記憶する記憶手段と；前記利用者識別データに関連して定められた暗証データを入力する暗証データ入力手段と；前記サービス提供要求ごとに暗号鍵を作成し、前記利用者識別データ及び前記暗証データを、前記暗号鍵を用いて暗号化する第1暗号化手段と；前記暗号化された利用者識別データ及び暗証データ、並びに前記暗号鍵を反映した暗号鍵情報から成る前記認証用情報の一部を含む第1データを前記受付端末へ伝達するとともに、前記認証用情報の残りを含む第2データを前記認証サーバへ伝達する伝達手段と；を備える構成とすることができる。

ここで、前記認証端末装置が、前記サービス提供システムから供給された公開鍵を用いて、前記暗号鍵を暗号化して前記暗号鍵情報を作成する第2暗号化手段を更に備える構成とすることができる。

また、前記認証端末装置が、前記サービス提供要求を特定するイベント識別データを生成するイベント識別データ生成手段を更に備える構成とし、前記第1データが前記イベント識別データを更に含むとともに、前記第2データが前記イベント識別データを更に含むこととすることができる。

この場合、前記伝達手段が、前記受付端末装置との間における第1の経路を介する通信を制御する第1通信制御部と；前記認証サーバとの間における、前記第1の経路とは異なる第2の経路を介する通信を制御する第2通信制御部と；を備える構成とすることができる。

そして、前記認証端末装置と前記受付端末装置との間の通信を近距離無線通信とし、前記認証端末装置と前記認証サーバとの間の通信を、移動体通信網を介した通信とすることができる。

また、前記受付端末装置が、前記認証端末装置との間の通信を制御する第3通信制御部と；前記認証端末装置から受信した前記第1データを含む受付データを作成する受付データ作成手段と；前記認証サーバとの間の通信を制御し、

前記受付データを前記受付サーバへ送信する第4通信制御部と；を備える構成とすることができる。

また、イベント識別データを使用する本発明の認証システムでは、前記認証端末装置が、前記第1データを画像パターンに変換する画像パターン作成装置を更に備え、前記伝達手段が、前記第1データが変換された画像パターンを表示する表示装置と；前記認証サーバとの間における通信を制御する第1通信制御部と；を備える構成とすることができる。

ここで、前記画像パターン作成装置が、前記認証サーバにから前記通信制御部を介して指定された手順に従って、前記第1データから前記画像パターンへの変換を行うこととすることができる。

また、受付端末装置が、前記認証端末装置の表示装置に表示された、前記第1データに応じた画像パターンを読み取って、前記第1データに変換する画像パターン読取手段と；前記第1データを含む受付データを作成する受付データ作成手段と；前記認証サーバとの間の通信を制御し、前記受付データを前記受付サーバへ送信する第2通信制御部と；を備える構成とすることができる。

また、本発明の認証システムでは、前記認証サーバとして本発明の認証サーバを使用することができる。すなわち、本発明の認証システムでは、前記認証サーバが、前記受付端末装置との間の通信を制御し、前記第1データを含む受付データを受信する第1データ通信制御部と；前記認証端末装置との間の通信を制御し、前記第2データを受信する第2データ通信制御部と；前記第1データと、前記第1データに含まれるイベント識別データと同一のイベント識別データを含む第2データとを1組のデータとして、前記1組のデータに含まれる前記暗号化された利用者識別データ及び暗証データを、前記1組のデータに含まれる暗号鍵情報を用いて復号化する復号化手段と；前記復号化手段により復号化された前記利用者識別データと前記暗証データとを照合し、前記取引者に関する認証を行う認証手段と；を備える構成とすることができる。

ここで、前記認証サーバが、前記認証端末装置が前記暗号鍵を暗号化して前記暗号鍵情報を作成する際に用いる公開鍵を、所定の個人鍵に基づいて作成し、前記第2データ通信制御装置を介して前記公開鍵を前記認証端末装置に供給する公開鍵作成手段を更に備える構成とし、前記復号化手段が、前記個人鍵を用いて前記暗号鍵情報を復号化し、復号化された前記暗号鍵を用いて、前記暗号化された利用者識別データ及び暗証データを復号化する構成とすることができる。

図面の簡単な説明

図1は、本発明の第1の実施形態に係る決済システムの構成を模式的に示す図である。

図2は、図1の認証端末装置の構成を示すブロック図である。

図3は、図1の受付端末装置の構成を示すブロック図である。

図4は、図1の決済サーバの構成を示すブロック図である。

図5は、本発明の第2の実施形態に係る決済システムの構成を模式的に示す図である。

図6は、図5の認証端末装置の構成を示すブロック図である。

図7は、図5の受付端末装置の構成を示すブロック図である。

図8は、図5の決済サーバの構成を示すブロック図である。

発明を実施するための最良の形態

《第1の実施形態》

以下、本発明の第1の実施形態を、図1～図4を参照して説明する。図1には、本発明の認証システムを適用した決済システム100の構成が模式的に示されている。この図1に示されるように、本実施形態の決済システム100は、決済サービスの提供の要求に応じて、サービス提供要求を行った利用者の認証

を行う認証サーバとしての機能を併せ持ち、決済の可否の判定を行う決済サーバ10と、店舗50内に設置され、決済サーバ10と公衆回線や専用回線等の有線電気通信回線31で接続された受付端末としての決済端末装置20とを備えている。

この決済システム100では、決済サーバ10が、有線電気通信回線32及び移動体通信基地局35を介して、決済サービスの利用者の一人が個人的に所有している移動体通信端末である認証端末装置80とも接続できるようになっている。すなわち、決済サーバ10は、移動体通信網における無線通信回線36を介して、認証端末装置80との間で通信可能となっている。

さらに、認証端末装置80と決済端末装置20との間では、近距離無線通信により、認証端末装置80から決済端末装置20へのデータの転送が可能となっている。

なお、図1では、店舗50内における決済端末装置20及び認証端末装置80の数を1つずつ示しているが、これらの数は1つずつに限定されず、それぞれが任意の数であってよい。また、図1では、決済端末装置20が設置される店舗50が1つのみ示されているが、店舗50の数は1つに限定されず、任意の数であってよい。

前記認証端末装置80は、図2に示されるように、(a)処理装置81と、(b)処理装置81からの表示指示データDPDに従って画面表示する表示装置82と、(c)サービス利用者希望者による操作によって、後述する暗証番号等のデータIPDを処理装置81に入力する入力装置83とを備えている。また、認証端末装置80は、(d)近距離無線通信による認証用データCTDの決済端末装置20への送信を制御する通信制御装置84と、(e)移動体通信網を介した通信による決済サーバ10への復号用データDCDの送信及び決済サーバ10からの公開鍵OPKの受信を制御する通信制御装置85とを更に備えている。

前記処理装置 8 1 は、(i) 認証端末装置 8 0 の全体を統括制御する制御装置 9 5 と、(ii) 決済サービスにおける利用者の識別子 U I D を記憶する記憶装置 9 1 と、(iii) 制御装置 9 5 による制御のもとで、サービス提供要求ごとに乱数発生により暗号鍵 C D K を生成し、その暗号鍵を用いて、記憶装置 9 1 から読み出した識別子データ U I D 及び入力装置 8 3 から入力データ I P D として入力された暗証番号 R C N を暗号化して、暗号化認証データ C R U を作成する第 1 暗号化装置 9 2 とを備えている。また、処理装置 8 1 は、(iv) 制御装置 9 5 による制御のもとで、決済サーバ 1 0 から移動体通信網を介して供給された公開鍵 O P K を用いて、第 1 暗号化装置 9 2 から供給された暗号鍵 C D K を暗号化し、暗号化暗号鍵データ C C K を作成する第 2 暗号化装置 9 3 と、(v) 制御装置 9 5 による制御のもとで、サービス提供要求ごとに、そのサービス提供要求を識別するためのイベント識別子 E I D を作成するイベント識別子作成装置 9 4 とを更に備えている。

ここで、制御装置 9 5 は、上記の認証端末装置 8 0 の統括制御に加えて、第 1 暗号化装置 9 2 から供給された暗号化認証データ C R U 及びイベント識別子作成装置 9 4 から供給されたイベント識別子 E I D を含む認証用データ C T D を作成し、通信制御装置 8 4 を介して決済端末装置 2 0 へ送信する。また、制御装置 9 5 は、第 2 暗号化装置 9 3 から供給された暗号化暗号鍵データ C C K 及びイベント識別子作成装置 9 4 から供給されたイベント識別子 E I D を含む復号用データ D C D を作成し、通信制御装置 8 5 を介して、決済サーバ 1 0 へ送信する。

なお、図 2 では、データの流が実線矢印により示され、また、処理装置 8 1 内における制御の流れが破線矢印によって示されている。

また、本実施形態では、上記のように各装置を組み合わせることで認証端末装置 8 0 を構成したが、認証端末装置 8 0 を計算機システムとして構成し、処理装置 8 1 の構成要素である第 1 暗号化装置 9 2、第 2 暗号化装置 9 3、イベント識

別子作成装置 9 4、及び制御装置 9 5 の機能を、計算機システムに内蔵されるプログラムによって実現することもできる。

また、利用者識別子 U I D は、決済サービスの提供に先立って、決済サーバ 1 0 含む決済サービス提供者からサービス利用可能者に通知される。この利用者識別子 U I D の通知を受けたサービス利用可能者は、入力装置 8 3 を操作して利用者識別子 U I D を記憶装置 9 1 に格納するようになっている。また、利用者識別子 U I D の通知を受けたサービス利用可能者は、その利用者識別子 U I D と対を成し、決済サービスにあたってのなりすましを防止するための暗証番号 R C N をサービス提供者へ通知しておくことが、決済サービスの提供を受けるための必須条件となっている。

前記決済端末装置 2 0 は、図 3 に示されるように、(a) 決済端末装置 2 0 の全体を統括制御する処理装置 2 1 と、(b) 処理装置 2 1 からの表示指示データ D P D' に従って画面表示する表示装置 2 2 と、(c) 決済端末装置 2 0 による操作によって、後述する商品代金等の決済データ F E D を処理装置 2 1 に入力する入力装置 2 3 とを備えている。また、決済端末装置 2 0 は、(d) 近距離無線通信による認証端末装置 8 0 からの認証用データ C T D の受信を制御する通信制御装置 2 4 と、(e) 有線通信回線 3 1 を介した通信による決済サーバ 1 0 への受付データ R C D の送信及び決済サーバ 1 0 からの決済結果データ S C R の受信を制御する通信制御装置 2 5 とを備えている。

ここで、処理装置 2 1 は、上記の認証端末装置 8 0 の統括制御に加えて、決済データ F E D 及び認証用データ C T D を含む受付データ R C D を作成し、通信制御装置 2 5 を介して、決済サーバ 1 0 へ送信する。なお、図 3 では、データの流れが実線矢印により示されている。

前記決済サーバは、図 4 に示されるように、(a) 処理装置 1 1 と、(b) 移動体通信網を介した通信による認証端末装置 8 0 への公開鍵 O P K の送信及び認証端末装置 8 0 からの復号用データ D C D の受信を制御する通信制御装置 1 2

と、(c)有線通信回線31を介した通信による決済端末装置20からの受付データRCDの受信及び決済端末装置20への決済結果データSCRの送信を制御する通信制御装置13とを備えている。

前記処理装置11は、(i)決済サーバ10の全体を統括制御するとともに、受付データRCD内のイベント識別子と復号用データDCD内のイベント識別子の照合を行う制御装置19と、(ii)制御装置19による制御のもとで、決済サーバ10として固有の個人鍵PSKとこの個人鍵PSKに基づいて作成された公開鍵OPKを記憶する記憶装置14と、(iii)制御装置19による制御のもとで、記憶装置14から読み出した個人鍵PSKを用いて、制御装置19から供給された、復号用データDCD内の暗号化暗号鍵データCCKを暗号鍵CDKに復号化する暗号鍵復号化装置15とを備えている。また、処理装置11は、(iv)制御装置19による制御のもとで、暗号鍵復号化装置15から供給された暗号鍵CDKを用いて、制御装置19から供給された暗号化認証データCRUを利用者識別子UID及び暗証番号RCNに復号化する認証データ復号化装置16と、(v)制御装置19による制御のもとで、認証データ復号化装置16から供給された利用者識別子UIDと暗証番号RCNとを照合することにより利用者の本人認証を行うとともに、本人認証が行われたとき、制御装置19から供給された、受付データRCD内の決済データに基づいて決済の可否の判定を行い、決済結果データSCRを作成する決済判定装置17とを更に備えている。

なお、図4では、図2の場合と同様に、データの流れが実線矢印により示され、また、処理装置11内における制御の流れが破線矢印によって示されている。

また、本実施形態では、上記のように各装置を組み合わせて決済サーバ10を構成したが、決済サーバ10を計算機システムとして構成し、処理装置11の構成要素である暗号鍵復号化装置15、認証データ復号化装置16、決済判

定装置 17、及び制御装置 19 の機能を、計算機システムに内蔵されるプログラムによって実現することもできる。

次に、以上のように構成された決済システム 100 による決済サービスの実施について、主に図 1 を参照するとともに、適宜他の図面を参照しつつ説明する。

なお、前提として、決済サーバ 10（より詳しくは、図 4 の記憶装置 14）には、個人鍵 P S K 及び公開鍵 O P K が記憶されているものとする。また、認証端末装置 80 には、決済サーバ 10 から公開鍵 O P K が供給されているものとする。更に、認証端末装置 80（より詳しくは、図 2 の記憶装置 91）には利用者識別子 U I D が記憶されているものとする。また、暗証番号 R C N は、決済サーバ 10（より詳しくは、図 4 の決済判定装置 17）に通知されているものとする。

店舗 50 において、サービス利用希望者が購入したい商品等を選び、それを決済端末装置 20 の操作者に示すと、該操作者は、決済端末装置 20 の入力装置 23（図 3 参照）を操作して、商品代金等の決済データ F E D を決済端末装置 20 に入力する。決済端末装置 20 は、入力した決済データ F E D に示された決済代金を表示装置 22（図 3 参照）に表示する。

サービス利用希望者は、表示装置 23 に表示された決済金額を確認後、認証端末装置 80 の入力装置 83（図 2 参照）を操作して、認証端末装置 80 を決済サービス提供要求モードに設定する。決済サービス提供要求モードに設定された認証端末装置 80 は、表示装置 82（図 2 参照）に暗証番号 R C N を入力することを促す表示をして、暗証番号 R C N の入力待ち状態となる。

引き続いてサービス利用希望者が入力装置 83 を操作して暗証番号 R C N を入力すると、認証端末装置 80（より詳しくは、図 2 の第 1 暗号化装置 92）は、今回の決済サービス提供要求についての暗号鍵 C D K を生成し、その暗号鍵 C D K を用いて利用者識別子 U I D 及び暗証番号 R C N を暗号化して、暗号

化認証データCRUを作成する。また、認証端末装置80（より詳しくは、図2の第2暗号化装置93）は、公開鍵OPKを用いて暗号鍵CDKを暗号化して、暗号化暗号鍵データCCKを作成する。さらに、認証端末装置80（より詳しくは、図2のイベント識別子作成装置94）は、今回のサービス提供要求を識別するためのイベント識別子EIDを作成する。

そして、認証端末装置80（より詳しくは、図2の制御装置95）は、暗号化認証データCRU及びイベント識別子EIDを含む認証用データCTDを作成して、近距離無線通信により決済端末装置20へ向けて送信する。また、認証端末装置80は、暗号化暗号鍵データCCK及びイベント識別子EIDを含む復号用データDCDを作成し、移動体通信網を介して、決済サーバ10へ向けて送信する。

認証用データCTDを受信した決済端末装置20は、認証用データCTD及び上述の決済データFEDを含む受付データRCDを作成する。そして、決済端末装置20は、有線通信回線31を介して、受付データRCDを決済サーバ10へ向けて送信する。

決済サーバ10は、受付データRCD及び復号用データDCDを非同期に受信する。かかる非同期に受信した受付データRCD及び復号用データDCDが、同一の決済サービス提供要求に係る対であることを特定するため、決済サーバ10（より詳しくは、図4の制御装置19）は、受付データに含まれるイベント識別子と復号用データに含まれるイベント識別子との照合を行う。この照合の結果、同一のイベント識別子EIDを含む受付データRCDと復号用データDCDとが、同一の決済サービス提供要求に係るものであると判定される。

こうして、同一のサービス提供要求に係る受付データRCD及び復号用データDCDが特定されると、決済サーバ10（より詳しくは、図4の暗号鍵復号化装置15）は、個人鍵PSKを用いて、復号用データDCDに含まれる暗号化暗号鍵データCCKを復号化し、暗号鍵CDKを得る。引き続き、決済サー

サーバ１０（より詳しくは、図４の認証用データ復号化装置１６）は、暗号鍵ＣＤＫを用いて、受付データＲＣＤに含まれる暗証化認証データＣＲＵを復号化し、利用者識別子ＵＩＤ及び暗証番号ＲＣＮを得る。

次に、決済サーバ１０（より詳しくは、図４の決済判定装置１７）は、利用者識別子ＵＩＤと暗証番号ＲＣＮとを照合することにより、サービス利用希望者がサービス利用可能者であるか否かを判定することにより、本人認証を行う。この本人認証が肯定的な結果であった場合には、受付データＲＣＤ内の決済データに基づいて決済の可否の判定を行う。この決済の可否の判定が肯定的な場合には、決済が行われる。引き続き、本人認証の結果及び決済可否の判定結果に応じて、「本人認証が否定的であった」、「本人認証は肯定的であったが、サービス利用可能者の残金不足等により決済ができなかった」、「本人認証が肯定的であり、決済が完了した」等を示す決済結果データＳＣＲが作成される。

そして、決済サーバ１０は、有線通信回線３１を介して、決済結果データＳＣＲを決済端末装置２０へ向けて送信する。

決済結果データＳＣＲを受信した決済端末装置２０は、決済結果を表示装置２２に表示して、サービス利用希望者に通知する。

以上説明したように、本実施形態の決済システム１００によれば、認証端末装置１０が、利用者識別子ＵＩＤ及び暗証番号ＲＣＮを、サービス提供要求ごとに作成した暗号鍵ＣＤＫを用いて暗号化し、暗号化された利用者識別子及び暗証番号を含む認証用データＣＴＤ、並びに暗号鍵ＣＤＫを公開鍵ＯＰＫにより暗号化した暗号化暗号鍵データＣＣＫを含む復号用データＤＣＤを、決済端末装置２０及び決済サーバを備えるサービス提供システムに送信する。そして、サービス提供システムにおいて、暗号鍵情報に基づいて、暗号化された利用者識別子及び暗証番号を復号化した後、復号化された利用者識別子ＵＩＤと復号化された暗証番号ＲＣＮとを照合して、利用者の認証を行い、決済を行う。したがって、利用者識別子ＵＩＤ及び暗証番号ＲＣＮといった本人認証用データ

を平文のまま送信することによるセキュリティの低下を防止することができる。
また、１つの暗号鍵を固定的に使用することによるセキュリティの低下を防止することができる。

また、暗証番号の入力をサービス利用者が個人的に保有する認証端末装置 １０を操作して行うので、従前のデビットカード決済における決済端末の操作による暗証番号の入力と比べて、盗み見による暗証番号の窃取の危険性を低減することができる。

また、サービス提供システムから供給された公開鍵 O P K を用いて、認証端末装置 ８０で使用した暗号鍵 C D K を暗号化して、サービス提供システムに送信するので、決済システム １００としてのセキュリティを更に向上することができる。

また、認証端末装置 ８０が、サービス提供要求を特定するイベント識別子 E I D を作成し、暗号化された利用者識別子及び暗証番号、並びにイベント識別子 E I D を含む認証用データ C T D を決済端末装置 ２０へ送信するとともに、暗号化暗号鍵 C C K 及びイベント識別子 E I D を含む復号用データ D C D を決済サーバ １０へ送信する。また、決済端末装置 ２０は、認証用データ C T D 及び決済データ F E D を含む受付データ R C D を決済サーバ １０へ送信する。そして、決済サーバ １０は、イベント識別子 E I D をキーとして、決済端末装置 ２０からの受付データ R C D と、認証端末装置 ８０からの復号用データ D C D との関連付けを行う。したがって、決済端末装置 ２０には、利用者識別子 U I D 及び暗証番号 R C N といった個人情報暗号化された状態で供給されるのみなので、店頭等に設置される決済端末装置 ２０からの利用者識別子 U I D や暗証番号 R C N の窃取を防止することができるとともに、確実に本人認証を行うことができる。

また、認証端末装置 ８０と決済端末装置 ２０との通信経路と、認証端末装置 ８０と決済サーバ １０との通信経路とを別経路とし、１つの通信経路からの情

報の窃取によっては、利用者識別子U I D及び暗証番号R C Nを悪用できる態様で窃取することができないので、認証に関するセキュリティを向上することができる。

なお、本実施形態では、認証端末装置80と決済端末装置20との通信を近距離無線通信で行い、認証端末装置80と決済サーバ10との通信を、移動体通信網を介して行うこととしたが、それぞれを別経路とすれば、本実施形態と種類が異なる通信経路を採用することができる。かかる場合においても、本実施形態と同様のセキュリティを達成することができる。

また、本実施形態では、認証端末装置80において、暗号鍵を、認証サーバの公開鍵を用いて暗号化して、この暗号化された暗号鍵を暗号鍵情報として認証サーバへ送信したが、認証用データと復号用データとを完全に別経路で送信する本実施形態のような場合には、暗号鍵の暗号化を省略しても高いセキュリティを達成することができる。

また、本実施形態では、認証端末装置80から決済端末装置20への認証用データの伝達を近距離無線通信により行ったが、認証端末装置80の表示装置82に認証用データに応じたバーコード等の画像パターンを表示することとし、この画像パターンを決済端末装置20が具備するバーコードリーダ等の画像パターン読取装置によって読み取ることとしてもよい。かかる場合にも、画像パターンが盗み見られることによる個人情報の漏洩等に対して高いセキュリティを維持することができる。なお、この場合には、認証用データの画像パターンへの変換のアルゴリズムを含む変換手順を指定したプログラムを、認証サーバ10から認証端末装置80へダウンロードすることとすることが可能である。かかるダウンロード方式を採用すると、通常の携帯電話が有する資源によって、認証端末装置80を実現することができる。

《第2の実施形態》

次に、本発明の第2の実施形態を、図5～図6を参照して説明する。なお、

本実施形態の説明にあたって、第１の実施形態と同一又は同等の要素には同一の符号を付し、重複する説明を省略する。

図５には、本発明の認証システムを適用した決済システム１００'の構成が模式的に示されている。この図５に示されるように、本実施形態の決済システム１００'は、決済サーバ１０'と、決済端末装置２０'と、認証端末装置８０'とを備えている。そして、決済サーバ１０'、決済端末装置２０'、及び認証端末装置８０'は、通信回線網３０を介して、通信可能となっている。

なお、図５では、決済端末装置２０'及び認証端末装置８０'の数を１つずつ示しているが、これらの数は１つずつに限定されず、それぞれが任意の数であってよい。

前記認証端末装置８０'は、図６に示されるように、図２に示される第１実施形態の認証端末装置８０と比べて、通信制御装置８４及び通信制御装置８５に代えて、(a)通信回線網３０を介した、認証用データＣＴＤの決済端末装置２０'への送信及び決済端末装置２０'からの決済データＦＥＤ、決済結果データＳＣＲ'の受信、並びに、決済サーバ１０'への復号用データＤＣＤの送信及び決済サーバ１０'からの公開鍵ＯＰＫの受信を制御する通信制御装置８６を備える点、及び、(b)制御装置９５'が、第１の実施形態の制御装置９５の機能に加えて、受信した決済結果データＳＣＲ'に示された決済結果を表示装置８２に表示する機能を有する点のみが異なる。かかる認証端末装置８０'は、パーソナルコンピュータシステム等の計算機システムとして構成することができる。

前記決済端末装置２０'は、図７に示されるように、図３に示される第１実施形態の決済端末装置２０と比べて、(a)通信制御装置２４及び通信制御装置２５に代えて、通信回線網３０を介した、認証端末装置８０'からの認証用データＣＴＤの受信及び決済データＦＥＤ、決済結果データＳＣＲ'の認証端末装置８０'への送信、並びに、決済サーバ１０'への受付データＲＣＤの送信

及び決済サーバ10'からの決済結果データSCRの受信を制御する通信制御装置26を備える点、及び、(b)処理装置21'が、第1の実施形態における処理装置21の機能に加えて、決済サーバ10'からの決済結果データSCRに示される決済結果の内容を決済結果データSCR'として認証端末装置80'へ送信する機能を有する点のみが異なる。かかる決済端末装置20'は、パーソナルコンピュータシステム等の計算機システムとして構成することができる。なお、本実施形態では、決済端末装置20'は、サイバーモールの一部であるものとする。

前記認証サーバ10'は、図8に示されるように、図4に示される第1実施形態の決済サーバ10と比べて、通信制御装置17及び通信制御装置18に代えて、通信回線網30を介した、認証端末装置80'への公開鍵OPKの送信及び認証端末装置80'からの復号用データDCDの受信、並びに、決済端末装置20'からの受付データRCDの受信及び決済端末装置20'への決済結果データSCRの送信を制御する通信制御装置18を備える点のみが異なる。

次に、以上のように構成された決済システム100'による決済サービスの実施について、主に図5を参照するとともに、適宜他の図面を参照しつつ説明する。

なお、前提として、第1の実施形態と同様に、決済サーバ10'には、個人鍵PSK及び公開鍵OPKが記憶されているものとする。また、認証端末装置80'には、決済サーバ10'から公開鍵OPKが供給されているものとする。更に、認証端末装置80'には利用者識別子UIDが記憶されているものとする。また、暗証番号RCNは、決済サーバ10'に通知されているものとする。

決済端末装置20'を備えるサイバーモールにおいて、サービス利用希望者が購入したい商品等を選び、それを決済端末装置20'に示すと、決済端末装置20'は、通信回線網30を介して、商品代金等の決済データFEDを認証端末装置10'に送信する。認証端末装置10'は、受信した決済データFE

Dに示された決済代金を表示装置 8 2 に表示する。

サービス利用希望者は、表示装置 8 2 に表示された決済金額を確認後、認証端末装置 8 0' の入力装置 8 3 を操作して、認証端末装置 8 0 を決済サービス提供要求モードに設定する。以後、第 1 の実施形態の場合と同様にして、サービス利用希望者による認証端末装置 8 0' への暗証番号の入力から、決済サーバ 1 0' から決済端末装置 2 0' への決済データ S C R の送信が行われる。

引き続き、決済データ S C R を受信した決済端末装置 2 0' は、表示装置 2 2 に決済結果を表示して、決済端末装置 2 0' の管理者に決済結果を示すとともに、決済データ S C R に示される決済結果の内容を決済結果データ S C R' として認証端末装置 8 0' へ送信する。

そして、決済結果データ S C R' を受信した認証端末装置 8 0' は、決済結果を表示装置 8 2 に表示して、サービス利用希望者に通知する。

本実施形態の決済システム 1 0 0' によれば、第 1 の実施形態の場合と同様に、利用者識別子 U I D 及び暗証番号 R C N といった本人認証用データを平文のまま送信することによるセキュリティの低下を防止することができる。また、1 つの暗号鍵を固定的に使用することによるセキュリティの低下を防止することができる。

また、第 1 の実施形態と同様に、公開鍵 O P K を用いて、認証端末装置 8 0' で使用した暗号鍵 C D K を暗号化するので、決済システム 1 0 0' としてのセキュリティを更に向上することができる。

また、第 1 の実施形態と同様に、決済端末装置 2 0' には、利用者識別子 U I D 及び暗証番号 R C N といった個人情報暗号化された状態で供給されるのみなので、店頭等に設置される決済端末装置 2 0' からの利用者識別子 U I D や暗証番号 R C N の窃取を防止できるとともに、確実に本人認証を行うことができる。

なお、上記の第 1 及び第 2 の実施形態では、本人認証用に利用者識別子と関

連付けられた暗証パスワードとして暗証番号を用いることとしたが、暗証パスワードは数字のみから構成される暗証番号に限定されず、数字以外の文字を含むこととしてもよい。

また、上記の第1及び第2の実施形態では、暗号鍵により暗号化された利用者識別子、暗号鍵により暗号化された暗証番号、及び公開鍵により暗号化された暗号鍵という3種のデータのうち、前暗号鍵により暗号化された利用者識別子及び暗号鍵により暗号化された暗証番号を認証端末装置から決済端末装置へ送信し、公開鍵により暗号化された暗号鍵を認証端末装置から決済サーバへ送信したが、これら3種のデータのうち、任意の1種又は2種のデータを認証端末装置から決済端末装置へ送信し、残りのデータを認証端末装置から決済サーバへ送信することにしても、上記の第1又は第2の実施形態の場合と同様のセキュリティ向上を図ることができる。

また、上記の第1及び第2の実施形態では、本発明を決済システムに適用した場合について説明したが、本発明は、本人認証を必要とする他の種類のシステムに適用することができ、個人情報のセキュリティを向上することができる。

産業上の利用可能性

本発明の認証端末装置、受付端末装置、認証サーバ、認証方法、及び認証システムは、利用者がサービスの提供を受けるにあたり、本人認証が必須となる場合に個人情報の漏洩を有効に防止することができるので、個人情報に対するセキュリティを向上したシステムの構築に利用することができる。

請 求 の 範 囲

1. サービスの利用者がサービス提供要求をするとき、前記利用者の認証用情報を、受付端末装置及び認証サーバを含むサービス提供システムへ向けて出力する認証端末装置であって、

前記利用者を特定するために予め定められた利用者識別データを記憶する記憶手段と；

前記利用者識別データに関連して定められた暗証データを入力する暗証データ入力手段と；

前記サービス提供要求ごとに暗号鍵を作成し、前記利用者識別データ及び前記暗証データを、前記暗号鍵を用いて暗号化する第1暗号化手段と；

前記暗号化された利用者識別データ及び暗証データ、並びに前記暗号鍵を反映した暗号鍵情報から成る前記認証用情報の一部を含む第1データを前記受付端末へ伝達するとともに、前記認証用情報の残りを含む第2データを前記認証サーバへ伝達する伝達手段と；を備える認証端末装置。

2. 請求項1に記載の認証端末装置において、

前記第1データは、前記暗号化された利用者識別データ及び暗証データを含む認証用データであり、

前記第2データは、暗号鍵情報を含む復号用データである。

3. 請求項1に記載の認証端末装置において、

前記サービス提供システムから供給された公開鍵を用いて、前記暗号鍵を暗号化して前記暗号鍵情報を作成する第2暗号化手段を更に備える。

4. 請求項 1 に記載の認証端末装置において、

前記サービス提供要求を特定するイベント識別データを生成するイベント識別データ生成手段を更に備え、

前記第 1 データは前記イベント識別データを更に含むとともに、前記第 2 データは前記イベント識別データを更に含み、

前記受付端末装置は、前記第 1 データを前記認証サーバへ送信する。

5. 請求項 1 に記載の認証端末装置において、

前記伝達手段は、

前記受付端末装置との間における第 1 の経路を介する通信を制御する第 1 通信制御部と；

前記認証サーバとの間における、前記第 1 の経路とは異なる第 2 の経路を介する通信を制御する第 2 通信制御部と；を備える。

6. 請求項 5 に記載の認証端末装置において、

前記受付端末装置との間の通信は、近距離無線通信であり、

前記認証サーバとの間の通信は、移動体通信網を介した通信である。

7. 請求項 1 に記載の認証端末装置において、

前記第 1 データを画像パターンに変換する画像パターン作成装置を更に備え、

前記伝達手段は、

前記第 1 データが変換された画像パターンを表示する表示装置と；

前記認証サーバとの間における通信を制御する第 1 通信制御部と；を備える。

8. 請求項 7 に記載の認証端末装置において、

前記画像パターン作成装置は、前記認証サーバにから前記第 1 通信制御部を介して指定された手順に従って、前記第 1 データから前記画像パターンへの変換を行う。

9. 請求項 5 に記載の認証端末装置との間で情報の伝達を行う受付端末装置であって、

前記認証端末装置との間の通信を制御する第 3 通信制御部と；

前記認証端末装置から受信した前記第 1 データを含む受付データを作成する受付データ作成手段と；

前記認証サーバとの間の通信を制御し、前記受付データを前記認証サーバへ送信する第 4 通信制御部と；を備える受付端末装置。

10. 請求項 7 に記載の認証端末装置との間で情報の伝達を行う受付端末装置であって、

前記認証端末装置の表示装置に表示された、前記第 1 データに応じた画像パターンを読み取って、前記第 1 データに変換する画像パターン読取手段と；

前記第 1 データを含む受付データを作成する受付データ作成手段と；

前記認証サーバとの間の通信を制御し、前記受付データを前記認証サーバへ送信する第 2 通信制御部と；を備える受付端末装置。

11. 請求項 4 に記載の認証端末装置との間で通信を行う認証サーバであって、

前記受付端末装置との間の通信を制御し、前記第 1 データを含む受付データを受信する第 1 データ通信制御部と；

前記認証端末装置との間の通信を制御し、前記第 2 データを受信する第 2 データ通信制御部と；

前記第 1 データと、前記第 1 データに含まれるイベント識別データと同一のイベント識別データを含む第 2 データとを 1 組のデータとして、前記 1 組のデータに含まれる前記暗号化された利用者識別データ及び暗証番号を、前記 1 組のデータに含まれる暗号鍵情報を用いて復号化する復号化手段と；

前記復号化手段により復号化された前記利用者識別データと前記暗証データとを照合し、前記取引者に関する認証を行う認証手段と；を備える認証サーバ。

1 2. 請求項 1 1 に記載の認証サーバにおいて、

前記認証端末装置が前記暗号鍵を暗号化して前記暗号鍵情報を作成する際に用いる公開鍵を、所定の個人鍵に基づいて作成し、前記第 2 データ通信制御装置を介して前記公開鍵を前記認証端末装置に供給する公開鍵作成手段を更に備え、

前記復号化手段は、前記個人鍵を用いて前記暗号鍵情報を復号化し、復号化された前記暗号鍵を用いて、前記暗号化された利用者識別データ及び暗証番号を復号化する。

1 3. 請求項 1 1 に記載の認証サーバにおいて、

前記認証端末装置との間の通信は、移動体通信網を介した通信である。

1 4. サービスの利用者による、受付端末装置及び認証サーバを含むサービス提供システムに対するサービス提供要求にあたり、前記利用者の認証を行う認証方法であって、

前記利用者が、予め定められた利用者識別データに関連して定められる暗証データを入力する暗証データ入力ステップと；

前記サービス提供要求ごとに、暗号鍵を生成する暗号鍵生成ステップと；

前記暗号鍵を用いて、前記利用者識別データ及び前記暗証データを暗号化する

る第1暗号化ステップと；

前記第1暗号化ステップにおいて暗号化された利用者識別データ及び暗証データ、並びに前記暗号鍵を反映した暗号鍵情報から成る認証用情報の一部を含む第1データを前記受付端末装置へ伝達するとともに、前記認証用情報の残りを含む第2データを前記認証サーバへ伝達する認証用情報伝達ステップと；

前記第1データを受けた前記受付端末装置が、前記第1データを含む受付データを前記認証サーバへ送信する受付データ送信ステップと；

前記第2データ及び前記受付データを受けた前記認証サーバが、前記利用者の認証を行う認証ステップと；を含む認証方法。

15. 請求項14に記載の認証方法において、

前記サービス提供システムから供給された公開鍵を用いて、前記暗号鍵を暗号化して前記暗号鍵情報を作成する第2暗号化ステップを更に含む。

16. 請求項14に記載の認証方法において、

前記サービス提供要求を特定するイベント識別データを生成するイベント識別データ生成ステップを更に含み、

前記第1データは前記イベント識別データを更に含むとともに、前記第2データは前記イベント識別データを更に含む。

17. 請求項16に記載の認証方法において、

前記認証ステップは、

前記認証サーバが、前記第1データと、前記第1データに含まれるイベント識別データと同一のイベント識別データを含む第2データとを1組のデータとして、前記1組のデータに含まれる前記暗号化された利用者識別データ及び暗証番号を、前記1組のデータに含まれる暗号鍵情報を用いて復号化する復号

化ステップと；

前記復号化ステップにおいて復号化された前記利用者識別データと前記暗証データとを照合する照合ステップと；を含む。

18. 請求項14に記載の認証方法において、

前記認証用情報伝達ステップでは、

前記第1データは、第1の経路を介して前記受付端末装置へ伝達され、

前記第2データは、前記第1の経路とは異なる第2の経路を介して前記認証サーバへ伝達される。

19. 請求項14に記載の認証方法において、

前記暗号鍵情報は、前記認証サーバにおいて管理される個人鍵に基づいて作成された公開鍵を用いて暗号化されたものであり、

前記復号化ステップでは、前記個人鍵を用いて前記暗号鍵情報を復号化し、復号化された前記暗号鍵を用いて、前記暗号化された利用者識別データ及び暗証番号を復号化する。

20. サービスの利用者によるサービス提供要求にあたり、前記利用者の認証を行う認証システムであって、

前記利用者を特定するために予め定められた利用者識別データ及び前記利用者識別データに関連して定められた暗証データを、前記サービス提供要求ごとに作成した暗号鍵を用いて暗号化し、前記暗号化された利用者識別データ及び暗証データ、及び前記暗号鍵を反映した暗号鍵情報から成る認証用情報の一部を含む第1データ、及び前記認証用情報の残りを含む第2データを伝達する認証端末装置と；

前記認証用データを受け、前記第1データを含む受付データを作成して送信

する受付端末装置と；

前記受付データ及び前記第 2 データを受け、前記暗号鍵情報に基づいて前記暗号化された利用者識別データ及び暗証データを復号化し、復号化された利用者識別データと復号化された暗証データとを照合して、前記利用者の認証を行う認証サーバと；を備える認証システム。

2 1. 請求項 2 0 に記載の認証システムにおいて、

前記第 1 データは、前記暗号化された利用者識別データ及び暗証データを含む認証用データであり、

前記第 2 データは、暗号鍵情報を含む復号用データである。

2 2. 請求項 2 0 に記載の認証システムにおいて、

前記認証端末装置は、

前記利用者を特定するために予め定められた利用者識別データを記憶する記憶手段と；

前記利用者識別データに関連して定められた暗証データを入力する暗証データ入力手段と；

前記サービス提供要求ごとに暗号鍵を作成し、前記利用者識別データ及び前記暗証データを、前記暗号鍵を用いて暗号化する第 1 暗号化手段と；

前記暗号化された利用者識別データ及び暗証データ、並びに前記暗号鍵を反映した暗号鍵情報から成る前記認証用情報の一部を含む第 1 データを前記受付端末へ伝達するとともに、前記認証用情報の残りを含む第 2 データを前記認証サーバへ伝達する伝達手段と；を備える。

2 3. 請求項 2 2 に記載の認証システムにおいて、

前記認証端末装置は、前記サービス提供システムから供給された公開鍵を用

いて、前記暗号鍵を暗号化して前記暗号鍵情報を作成する第2暗号化手段を更に備える。

24. 請求項22に記載の認証システムにおいて、

前記認証端末装置は、前記サービス提供要求を特定するイベント識別データを生成するイベント識別データ生成手段を更に備え、

前記第1データは前記イベント識別データを更に含むとともに、前記第2データは前記イベント識別データを更に含む。

25. 請求項24に記載の認証システムにおいて、

前記伝達手段は、

前記受付端末装置との間における第1の経路を介する通信を制御する第1通信制御手段と；

前記認証サーバとの間における、前記第1の経路とは異なる第2の経路を介する通信を制御する第2通信制御部と；を備える。

26. 請求項25に記載の認証システムにおいて、

前記認証端末装置と前記受付端末装置との間の通信は、近距離無線通信であり、

前記認証端末装置と前記認証サーバとの間の通信は、移動体通信網を介した通信である。

27. 請求項25に記載の認証システムにおいて、

前記受付端末装置は、

前記認証端末装置との間の通信を制御する第3通信制御部と；

前記認証端末装置から受けた前記第1データを含む受付データを作成する

受付データ作成手段と；

前記認証サーバとの間の通信を制御し、前記受付データを前記受付サーバへ送信する第4通信制御部と；を備える。

28. 請求項24に記載の認証システムにおいて、

前記認証端末装置は、前記第1データを画像パターンに変換する画像パターン作成装置を更に備え、

前記伝達手段は、

前記第1データが変換された画像パターンを表示する表示装置と；

前記認証サーバとの間における通信を制御する第1通信制御部と；を備える。

29. 請求項28に記載の認証システムにおいて、

前記画像パターン作成装置は、前記認証サーバにから前記通信制御部を介して指定された手順に従って、前記第1データから前記画像パターンへの変換を行う。

30. 請求項28に記載の認証システムにおいて、

受付端末装置は、

前記認証端末装置の表示装置に表示された、前記第1データに応じた画像パターンを読み取って、前記第1データに変換する画像パターン読取手段と；

前記第1データを含む受付データを作成する受付データ作成手段と；

前記認証サーバとの間の通信を制御し、前記受付データを前記受付サーバへ送信する第2通信制御部と；を備える。

31. 請求項20に記載の認証システムにおいて、

前記認証サーバは、

前記受付端末装置との間の通信を制御し、前記第 1 データを含む受付データを受信する第 1 データ通信制御部と；

前記認証端末装置との間の通信を制御し、前記第 2 データを受信する第 2 データ通信制御部と；

前記第 1 データと、前記第 1 データに含まれるイベント識別データと同一のイベント識別データを含む第 2 データとを 1 組のデータとして、前記 1 組のデータに含まれる前記暗号化された利用者識別データ及び暗証番号を、前記 1 組のデータに含まれる暗号鍵情報を用いて復号化する復号化手段と；

前記復号化手段により復号化された前記利用者識別データと前記暗証データとを照合し、前記取引者に関する認証を行う認証手段と；を備える。

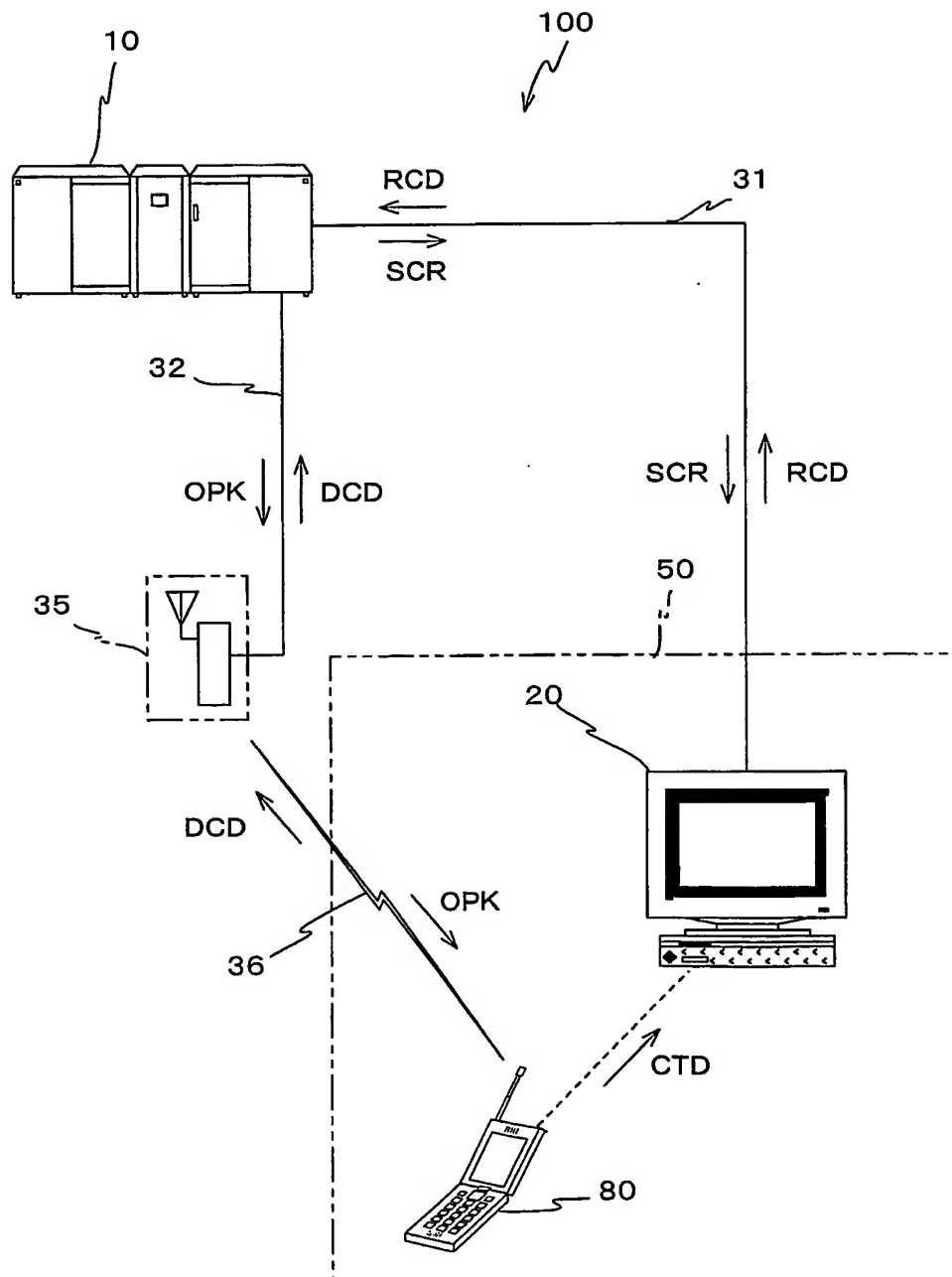
3 2. 請求項 3 1 に記載の認証システムにおいて、

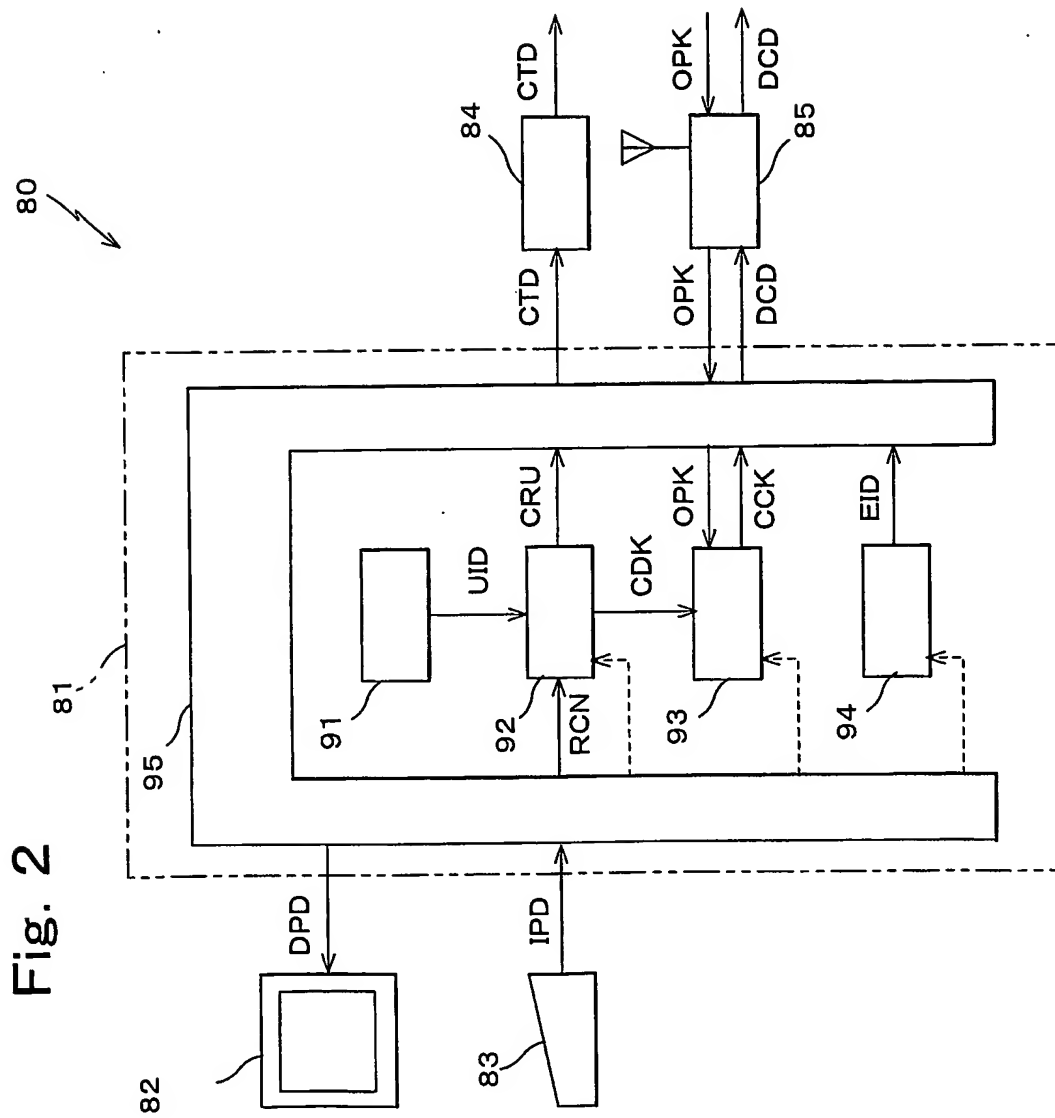
前記認証サーバは、前記認証端末装置が前記暗号鍵を暗号化して前記暗号鍵情報を作成する際に用いる公開鍵を、所定の個人鍵に基づいて作成し、前記第 2 データ通信制御装置を介して前記公開鍵を前記認証端末装置に供給する公開鍵作成手段を更に備え、

前記復号化手段は、前記個人鍵を用いて前記暗号鍵情報を復号化し、復号化された前記暗号鍵を用いて、前記暗号化された利用者識別データ及び暗証番号を復号化する。

1 / 8

Fig. 1





3 / 8

Fig. 3

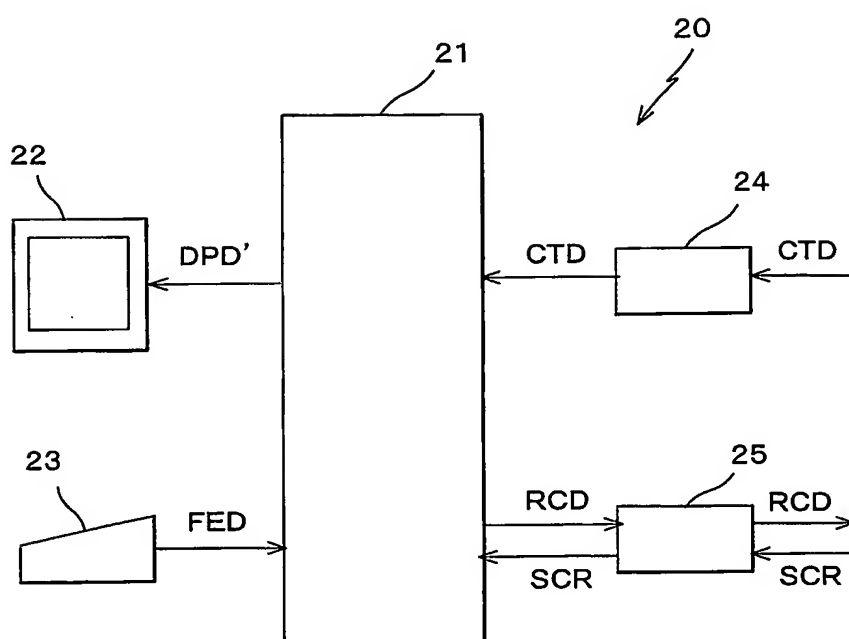
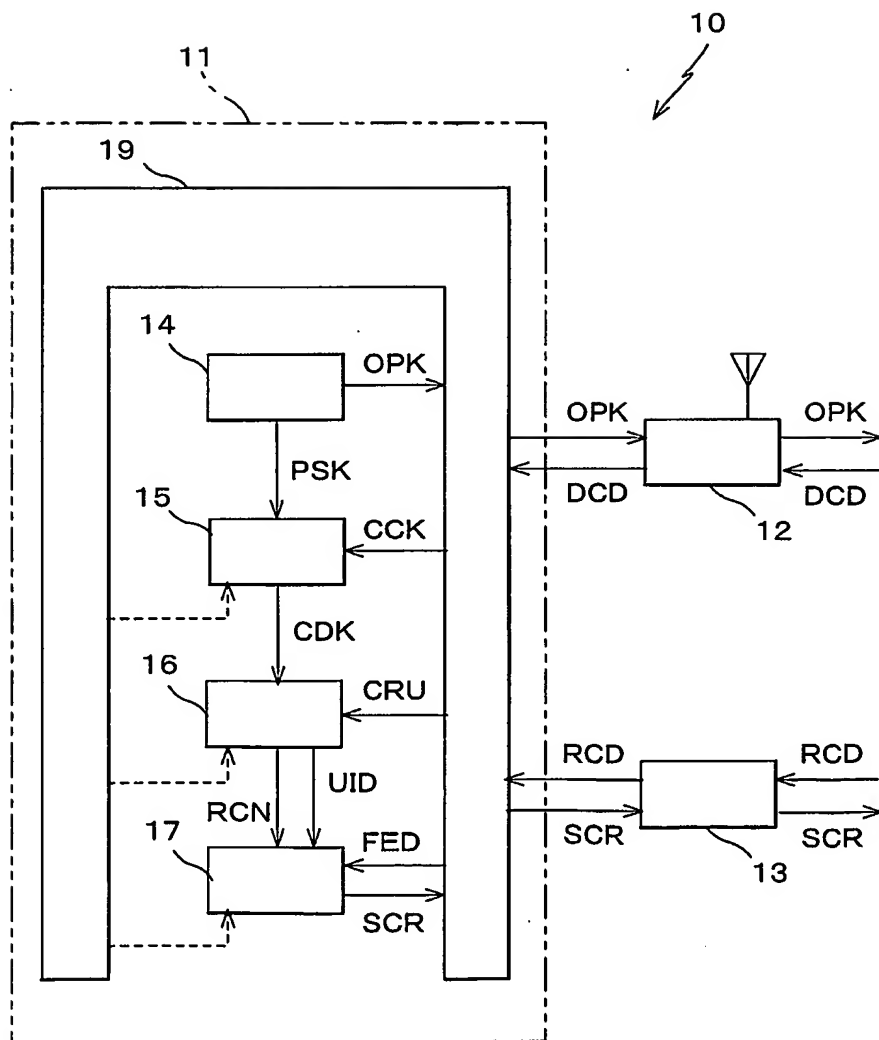
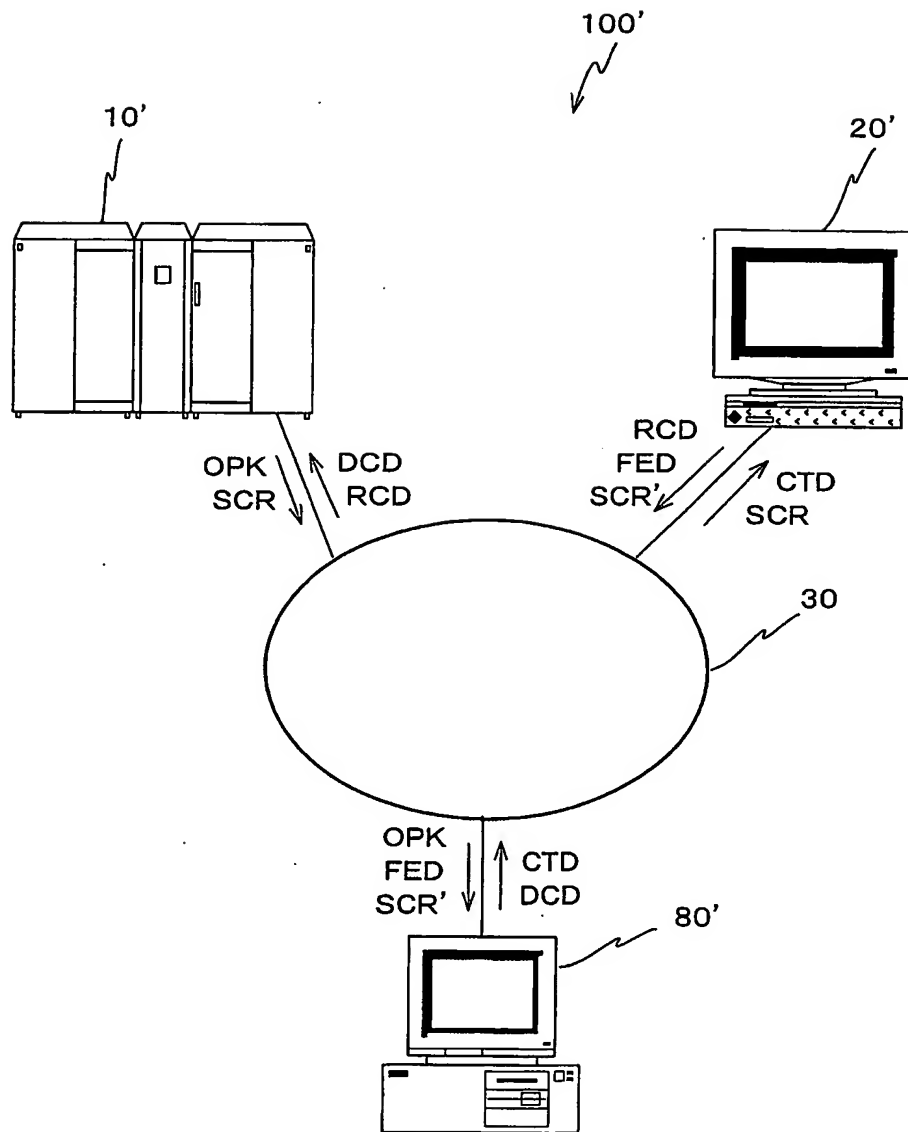


Fig. 4



5 / 8

Fig. 5



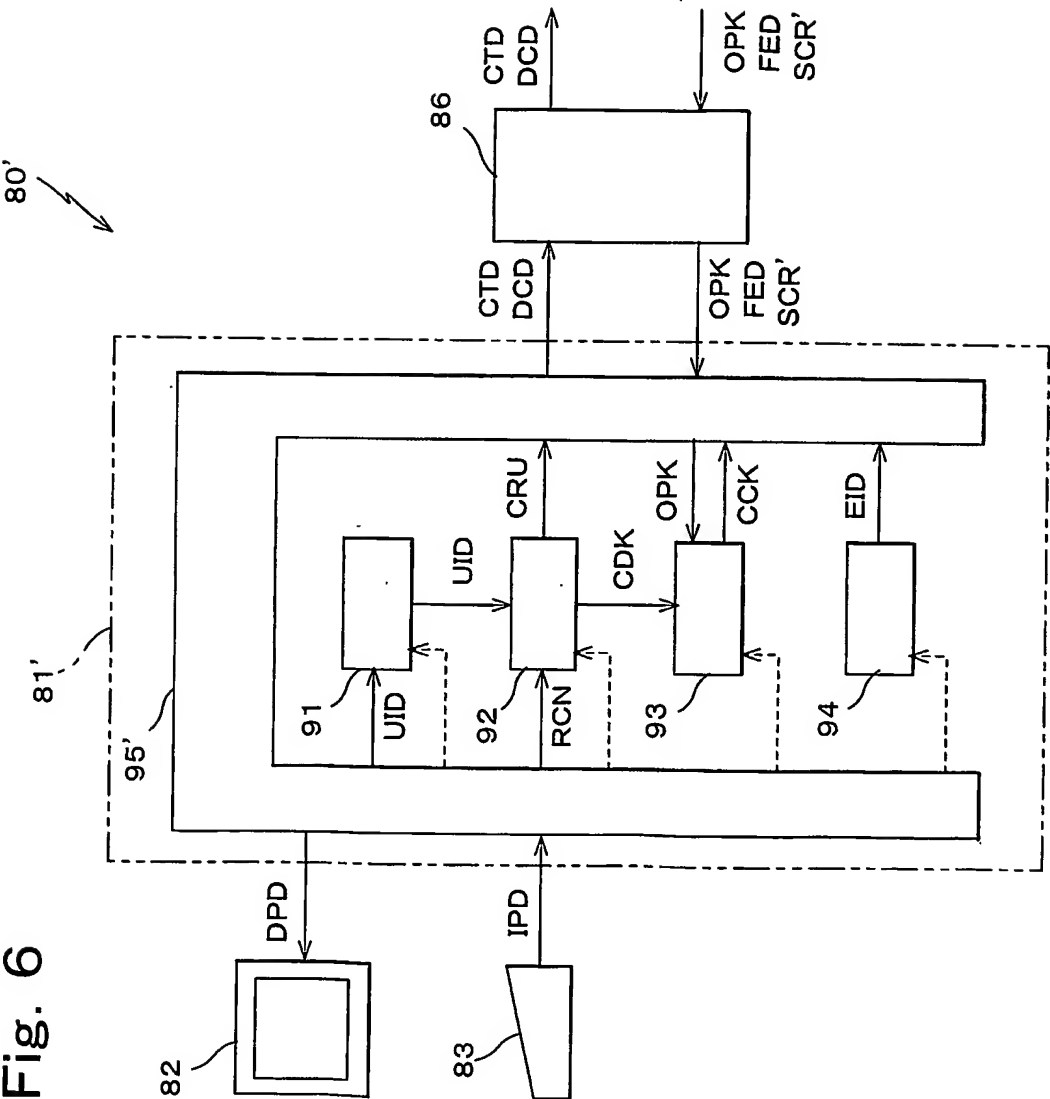


Fig. 6

7 / 8

Fig. 7

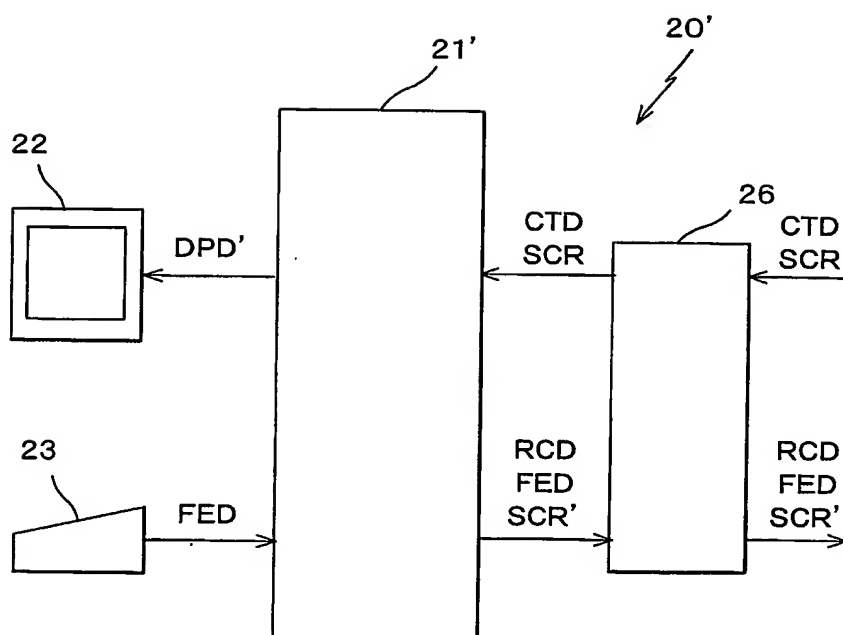
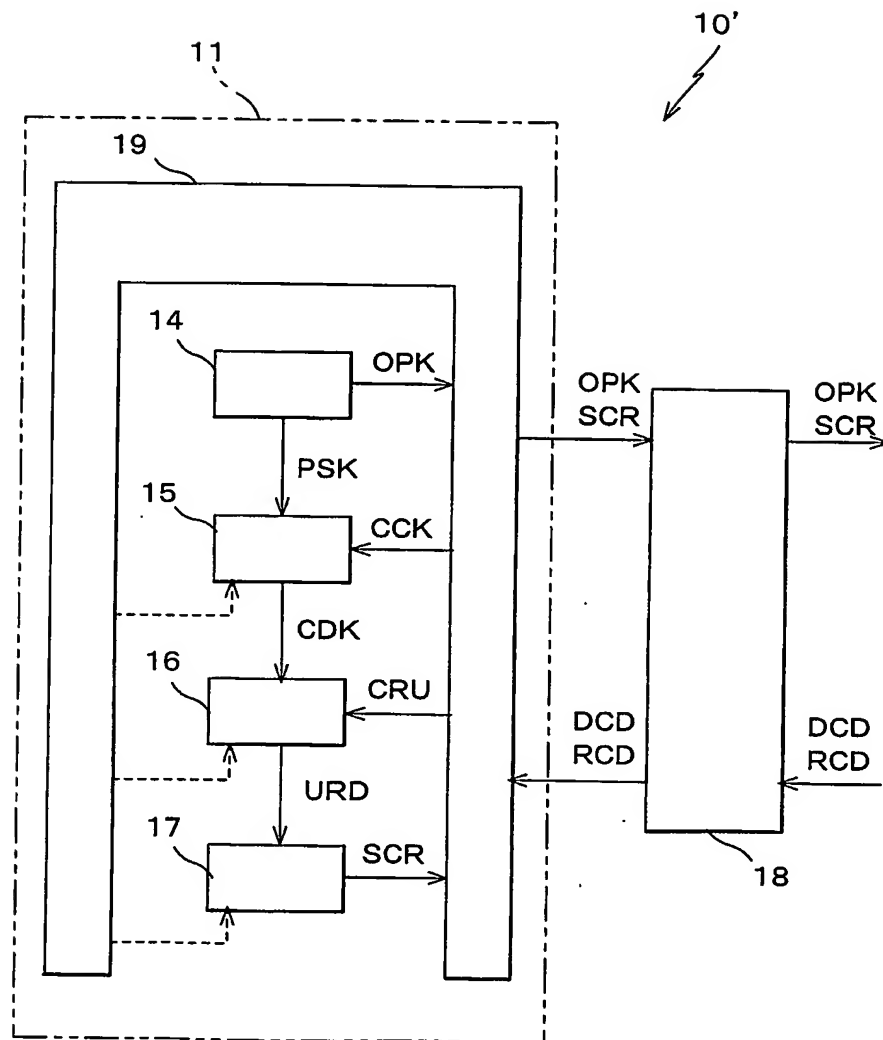


Fig. 8



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/08010

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.⁷ G06F 15/00, H04L 9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ G06F 15/00, G06F 17/60, G06K 19/00, H04K 1/00, H04L 9/00, G09C 1/00, H04Q 7/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Jitsuyo Shinan Toroku Koho	1996-2001
Kokai Jitsuyo Shinan Koho	1971-2001	Toroku Jitsuyo Shinan Koho	1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-340255 A (Kyushu Nippon Denki Software K.K.), 22 December, 1998 (22.12.98), Full text; all drawings (Family: none)	1-32
Y	JP 9-307542 A (Sony Corporation), 28 November, 1997 (28.11.97), Par. Nos. [0041] to [0043]; Fig. 11 & WO 97/034279 A1 & EP 833294 A1	1-32
Y	JP 10-198739 A (Matsushita Electric Ind. Co., Ltd.), 31 July, 1998 (31.07.98), Par. Nos. [0114] to [0182]; Figs. 1, 2, 3, 6 & WO 98/021677 A1 & CN 1212773 A & EP 910028 A1	1-32
Y	JP 8-96043 A (AT & T Corporation), 12 April, 1996 (12.04.96), Full text; all drawings & CA 2156206 A & CA 2156206 A1 & EP 708547 A2 & US 5608778 A1	1-32

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
10 December, 2001 (10.12.01)Date of mailing of the international search report
18 December, 2001 (18.12.01)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/08010

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-155170 A (Toyo Communication Equipment Co., Ltd.), 09 June, 1998 (09.06.98), Full text; all drawings (Family: none)	7, 8, 10, 28-30

A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int. Cl ⁷ G06F 15/00, H04L 9/32		
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int. Cl ⁷ G06F 15/00, G06F 17/60, G06K 19/00, H04K 1/00, H04L 9/00, G09C 1/00, H04Q 7/00		
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1926-1996年 日本国公開実用新案公報 1971-2001年 日本国実用新案登録公報 1996-2001年 日本国登録実用新案公報 1994-2001年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 10-340255 A(九州日本電気ソフトウェア株式会社) 22.12月.1998 (22.12.98), 全文, 全図 (ファミリーなし)	1-32
Y	JP 9-307542 A(ソニー株式会社) 28.11月.1997 (28.11.97), 第0041-0043段落, 第11図 & WO 97/034279 A1 & EP 833294 A1	1-32
Y	JP 10-198739 A(松下電器産業株式会社) 31.7月.1998 (31.07.98), 第0114-0182段落, 第1, 2, 3, 6図 & WO 98/021677 A1 & CN 1212773 A & EP 910028 A1	1-32
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」特に関連のある文献ではなく、一般的技術水準を示すもの 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」口頭による開示、使用、展示等に関する文献 「P」国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」同一パテントファミリー文献		
国際調査を完了した日 10.12.01	国際調査報告の発送日 18.12.01	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 谷口 信行 電話番号 03-3581-1101 内線 3545	5B 9467

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 8-96043 A(エイ・ティ・アンド・ティ・コーポレーション) 12.4月.1996 (12.04.96) , 全文, 全図 & CA 2156206 A & CA 2156206 A1 & EP 708547 A2 & US 5608778 A 1	1-32
Y	JP 10-155170 A(東洋通信機株式会社) 9.6月.1998 (09.06.98) , 全文, 全図 (ファミリーなし)	7, 8, 10, 28-30